UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/559,414	04/26/2000	Greg Rosenberg	3974-4001	1221

3490 7590 04/20/2006

DOUGLAS T. JOHNSON
MILLER & MARTIN
1000 VOLUNTEER BUILDING
832 GEORGIA AVENUE
CHATTANOOGA, TN 37402-2289

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/20/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/559,414	ROSENBERG, GREG	
	Examiner	Art Unit	
	Syed Zia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This office action is in response to argument filed on January 30, 2006. Original application contained Claims 1-45. Applicant previously amended Claims 1, 29, 32, and 42. Applicant's request for reconsideration of the finality of the rejection of the last Office action is persuasive and, therefore, the finality of that action is withdrawn. Therefore, presently pending claims are 1-45.

Response to Arguments

Applicant's arguments with respect to claim 1-45 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 24is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: Applicant claimed that the first, second, third, fourth remote computers can be the same or different computer. If the computer is same then necessary step to

implement the invention should be different than when the computers are different. Either clarification or steps are required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 8-16, 25-29, 31, 36-40, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable by Brisbee et al, hereinafter Brisbee (U. S. Parent No: 6,963,971) in view of Ganesan (U. S. Parent No: 5,535,276).

As per claim 1, 25, and 36, Brisbee teaches a method of signing and authenticating electronic documents comprising securely storing a plurality of private keys associated with a plurality of users in a private key database on a local-computer cluster; receiving at the local computer cluster a signing request transmitted from a first remote computer by a first user; identifying the signing request as one transmitted by the first user, and identifying a signature ready document to be signed; retrieving at the local computer cluster the signature ready document to be signed; signing the signature ready document on the local computer cluster using a complete private key to produce a signed document (col. 7 line 34 to col.8 line 3).

Brisbee does not use of a pre-installed add-in software program configure to provide a signed message at the remote computer; therefore the newly added negative limitation is met.

Brisbee is silent in expressly disclosing storing private key portions and retrieving at the local computer cluster a private key portion associated with the first user from the private key database generating a complete private key using the retrieved private key portion if the retrieved private key portion is not a complete private key.

However, Ganesan teaches: securely storing a plurality of private key portions associated with a plurality of users in a private key database on a local computer cluster (column 8, lines 11-43); retrieving at the local computer cluster a private key portion associated with the first user (column 11, lines 29-31) from the-private key database generating a complete private key using the retrieved private key portion if the retrieved private key portion is not a complete private key (column 12, lines 45 to lines 53). Ganesan teaches that it is advantageous for a trusted third party to maintain one portion of every user's RSA private key (column 3, lines 17-25). This forces the user to interact with a trusted third party, which provides practical advantages such as instant revocation.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Ganesan within the system of Brisbee because interacting with a trusted third party by allowing it to do the signing would not only improve the overall trust of the system to all parties involved, but will also provide enhances security communication in conventional authentication system. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success because of known advantages of asymmetrical crypto-keys (col.7 line 35 to line 60).

As per claim 2, Brisbee teaches the private key portion is a complete private key (Fig.2, col. 4, line 1 to line 15).

As per claim 3, Brisbee teaches receiving signing identification credentials from the first user (col. 5 line 1 to line 7). Brisbee fails to teach constructing a complete private key using the private key portion and the received signing identification credentials. Ganesan teaches constructing a complete private key using the private key portion and the received signing identification credentials (column 12, lines 45-65 and column 14, lines 10-40). The examiner supplies to same rationale for the motivation to incorporate the teachings of Ganesan within-the system of Brisbee -as recited-in-the rejection of claim 1. Brisbee teaches sending identification credentials to the server. Furthermore, it would have been obvious to one of ordinary skill in the art to generate the server side of the private key with identifying credentials because it associates the key with the intended user.

As per claim 4, Brisbee is silent in disclosing transmitting over the Internet. Brisbee does teach a system communicating over a network (Fig.1-2). In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Brisbee to include communication over the Internet because the widely accessibility of network resources .

As per claims 8, 26, and 37, Brisbee teaches storing the signature ready document in a first document database (col. 6, line 58 to col.7 line 2).

As per claims 9 and 31, Brisbee teaches prior to signing: receiving form data from the first remote computer; and modifying the retrieved signature ready document based on the received form data (col. 6, lines 19 to line 39).

As per claims 10 and 27, Brisbee teaches the first document database is located on the local cluster (Fig.3).

As per claim 11, Brisbee teaches the first document database is located on a secure second remote computer for redundancy (Fig.3-4, and col.7 line 55 to line 65)).

As per claims 12, 28, and 38, Brisbee teaches storing the signed document in a second document database (col. 8 , lines 13 to line 44).

As per claims 13 and 29, Brisbee teaches the second database is located on a secure second computer remote computer (col. 7, line 23 to line 33).

As per claim 14, Brisbee teaches the second database is located on the local computer cluster (col. 7, line 34 to line 41).

As per claims 15 and 39, Brisbee teaches associating at least one of the signature ready document and the signed document with a document owner (col. 7, line 34 to line 54).

As per claims 16 and 40, Brisbee teaches notifying at least one of document owner and the first user that a signature ready document or a signed document has been signed (col. 7, line 34 to line 54).

As per claim 44, Brisbee teaches the first user is a registered user (col. 8 line 4 to line 11).

Claims 5-7,17-21, 23, 30, 32-35, 41, 42, 43, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over the system of Brisbee and Ganesan as applied to claims 1 and 17 above, and further in view of Smithies et al (U. S. Patent 5,544,255).

As per claims 5, 7, 32, Brisbee is silent in expressly teaching the use of web browser and hypertext markup languages to send signing request. Smithies teach a commerce system that utilizes the WWW to securely transmit documents with Web browsers using HTML (see col. 41, line 64-col. 43, line 10). The infrastructure on which Smithies bases his system in well known in the art, i.e. the WWW. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Smithies within the system of Brisbee and Ganesan because the Internet is network connecting the world and the main language of communicating is HTML for Web services.

As per claims 6 and 33, Brisbee teaches the retrieving at the local computer cluster the signature ready document is automatic (col. 6, lines 4 to line 10).

As per claims 17, 18, 41, and 42, the system of Brisbee and Ganesan teaches registering individuals as users, wherein registering includes: verifying and recording the identity of individuals registering (Brisbee: col. 3, line 35 to line 57,and col.7line34 to line 54) .

Brisbee does not explicitly teach associating passwords with the recorded digitized handwritten signatures and the recorded identities; and storing the recorded digitized handwritten signatures, and the recorded identities in an identity database, the identity database being accessible to the local computer cluster.

Smithies et al teach digitizing and recording handwritten signatures of individuals registering (column 3, line 35-column 4, lines 58); associating passwords with the recorded digitized handwritten signatures and the recorded identities (column 17, lines 14-21); and storing the recorded digitized handwritten signatures, and the recorded identities in an identity database,

the identity database being accessible to the local computer cluster (column 5, lines 5-12). The combined teachings of the system of Brisbee and Ganesan and Ganesan rely on a trusted server to perform the authentication process to allow access to a resource such as a document. Ganesan teaches authenticating a user to a trusted server (column 8, lines 3334). Smithies et al teach a method whereby a user can authenticate himself or herself to a remote computer system, thereby allowing access to a particular electronic document (column 6, lines 29-44). Smithies et al teach a signature can be transmitted to a remote site for verification before allowing access to a computer system and that the computer system can verify a handwritten signature. Therefore, a handwritten signature is a way in which a computer system can grant authentication to a user who has registered.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Smithies within the combined system of the of Brisbee and Ganesan because the use of digital handwritten signatures or any authenticating measurement is a way that a trusted server can viably authenticate a user. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claims 19 and 43, the Brisbee teaches the authenticating and identifying measurements can determine whether individuals have previously registered. This is an obvious conclusion to using personal identification number to identify a user as taught in col. 3, lines 49 to line 56, and col.6line 40 to line 49).

As per claims 20, Brisbee teaches the first user is a registered user (col. 8, lines 4 to line 11).

As per claims 21 and 45, Brisbee teaches appending a signature to a document (col.4 line 16 to line 26) but does not teach a digitized handwritten signature. Smithies et al teach appending the first user's digitized signature to the signature ready document; making a hash of the signature ready document; and encrypting the hash of the signature read), document with the first user's private key (column 20, lines 23-64 and column 13, lines 36-56). The examiner supplies the same rationale for the motivation as recited in the rejection of claim 17 to incorporate the use of a digitized signature as means to authenticate. Smithies et al teach hashing the signature and encrypting the hash with the user's key to further insure that the signed document cannot be altered or duplicated. Therefore, it would be advantageous to take these extra-steps to insure the validity of a signed document.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Smithies et al within the combined system of Brisbee and Ganesan because one would want to protect a signed document from being altered or duplicated (Brisbee col.1 line 45 to line 55). One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

As per claim 23, Brisbee teaches receiving signing identification credentials from the first user (col. 6 line 19 to line 39, and col.7line 34 to col.8 line 3). Brisbee fails to teach generating the private key portions for individuals registering, wherein the private key portions can be used with signing identification credentials to construct complete private keys; associating the generated private key portions with the recorded identities of individuals registering storing private key portions in a private key database. Ganesan teaches generating the private key

portions for individuals registering, wherein the private key portions can be used with signing identification credentials to construct complete private keys (column 12, lines 45-65 and column 14, lines 10-40); associating the generated private key portions with the recorded identities of individuals registering (column 14, lines 10-40); and storing private key portions in a private key database (column 8, lines 11-43 and column). The examiner supplies to same rationale for the motivation to incorporate the teachings of Ganesan within the system of Brisbee as recited in the rejection of claim 1. Brisbee teaches sending identification credentials to the server (col.5 line 65 to col.6 line 10). Furthermore, it would have been obvious to one of ordinary skill in the art to generate the server side of the private key with identifying credentials because it associates the key with the intended user.

As per claim 30, Brisbee teaches the local computer cluster further comprises a second memory device having stored thereon an identity database (col. 7 line 55 to col.8 line 3), the identity database including recorded user identities associated with signatures but is silent in disclosing user digitized handwritten signatures and passwords associated with the user identities. Smithies et al teach the identity database includes user digitized handwritten signatures and passwords associated with the user identities (column 17, lines 14-20). Smithies et al use this teaching in order to organize its users and their respective identifying information so that the system can correctly link and identify a user with his/her data as a way to authenticate. Brisbee stores the signed documents in a database with some identifying information (Fig.3) but not to the extent that Smithies et al teach. It would be advantageous to the system of Brisbee to

provide a more secure means to authenticate a person before the system allows a user to view a signed document. Smithies et al teachings provide such a means.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Smithies within the combined system of Brisbee and Ganesan because it would allow the system to have a more secure method of authentication. Ones skilled in the art would have been motivated to generate the-claimed invention with a reasonable expectation of success.

As per claim 34, Brisbee teaches a registration computer connected to the local computer cluster (Fig.3-4).

As per claim 35 Brisbee teaches registering individuals as users, wherein registering includes: verifying and recording the identity of individuals registering (col. 7 line 34 to col. 8 line 3). Brisbee does not explicitly teach digitizing and recording handwritten signatures (which is an example of a biometric measurement) of individuals registering; associating passwords with the recorded digitized handwritten signatures and the recorded identities; and storing the recorded digitized handwritten signatures, and the recorded identities in an identity database, the identity database being accessible to the local computer cluster. Smithies et al teach digitizing and recording handwritten signatures of individuals registering (column 3, line 35-column 4, lines 58); associating passwords with the recorded digitized handwritten signatures and the recorded identities (column 17, lines 14-21); and storing the recorded digitized handwritten signatures, and the recorded identities in an identity database, the identity database being

accessible to the local computer cluster (column 5, lines 5-12). The combined teachings of Brisbee and Ganesan rely on a trusted server to perform the authentication process to allow access to a resource such as a document. Ganesan teaches authenticating a user to a trusted server (column 8, lines-33-34): Smithies teach a-method-whereby a user can authenticate himself or herself to a remote computer system, thereby allowing access to a particular electronic document (column 6, lines 29-44). Smithies et al teach a signature can be transmitted to a remote site for verification before allowing access to a computer system and that the computer system can verify a handwritten signature. Therefore, a handwritten signature is a way in which a computer system can grant authentication to a user who has registered.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Smithies et al within the combined system of Brisbee and Ganesan because digital handwritten signature are a way that a trusted server can viably authenticate a user. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

Claims 24 is rejected under 35 U.S.C. 103(a) as being unpatentable by Brisbee and Ganesan and further in view of Smithies.

As per claim 24, Brisbee teaches transmitting user identification information and document identification information to the local computer cluster; transmitting a signing request to the local computer cluster from the remote computer independent of both a private key portion and a public key portion, the-signing request requesting the local computer cluster to retrieve the identified document from a second remote computer, obtaining a private encryption key

associated with the user from a third computer, and to sign the retrieved document using the obtained private key on a fourth computer, wherein the first, second, third, fourth remote computers can be the same or different computer (col.7line 33 tocol.8 line 3).

Brisbee is silent in disclosing running a browser on the first remote computer and using the browser to connect. Smithies teach a commerce system that utilizes the WWW to securely transmit documents with Web browsers using HTML (see col. 41, line 64-col. 43, line 10). The infrastructure on which Smithies bases his system in well known in the art, i.e. the WWW. In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Smithies within the system of Brisbee and Ganesan because the Internet is network connecting the world and the main language of communicating is HTML for Web services.

Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Brisbee, Ganesan, Smithies as applied to claims 1 and 17 above, and further in view of Shin (U. S. Patent 6,351,634).

As per-claim 22, Brisbee is-silent in disclosing: associating and storing a secret set of recognition graphics with the passwords in the identity database; displaying a plurality of recognition graphics, including recognition graphics from the secret set, on the first remote computer; requesting the first user to select graphics included in the secret set using a non-keyboard selecting device attached to the first remote computer; receiving a message from the first remote computer identifying the selected graphics; authorizing access to the local computer cluster if the selected graphics are included in the secret set.

However, Shin discloses:

associating and storing a secret set of recognition graphics with the passwords in the identity database (column 1, line 60-column 3, line 21);

displaying a plurality of recognition graphics, including recognition graphics from the secret set, on the first remote computer (column 1, line 60 column 3, line 21);

requesting the first user to select graphics included in the secret set using a non-keyboard selecting device attached to the first remote computer (column 1, line 60-column 3, line 21);

receiving a message from the first remote computer identifying the selected graphics (column 1, line 60-column 3; line 21); authorizing access to the local computer cluster if the selected graphics are included in the secret set (column 1, line 60-column 3, line 21).
Shin teaches that his method of authentication is better than methods using just keypad data entries. He suggests it is harder for someone to gain knowledge of a secret symbol than gaining knowledge of keypad alphanumeric passwords. Therefore, it would be advantageous to the overall security of the system is authentication was assisted by determining secret symbols as opposed to just alphanumeric passwords.

In view of this, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teaching of Shin within the combined system of Brisbee and Ganesan and Smithies because it would allow the system to have a more secure method of authentication. One skilled in the art would have been motivated to generate the claimed invention with a reasonable expectation of success.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Syed Zia whose telephone number is 571-272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SZ

April 14, 2006